524,625

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010395 A1

(51) International Patent Classification[7]: G08B 13/22, 13/00, G08C 17/00

(21) International Application Number: PCT/AU2003/000940

(22) International Filing Date: 24 July 2003 (24.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2002950343 24 July 2002 (24.07.2002) AU

(71) Applicant *(for all designated States except US)*: **EVATAY-HOW HOLDINGS PTY LTD** [AU/AU]; 8 Weir Street, Glen Iris, Victoria 3146 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAN DONGEN, Charles, Corneles** [AU/AU]; 4 Chamouni Court, Frankston, Victoria 3199 (AU). **HOWARD, Grover, Latham** [US/AU]; 807/14 Kavanagh Street, Melbourne, Victoria 3006 (AU). **CHAMPION, Lindsay, Alfred** [AU/AU]; 1 Grigg Avenue, Vermont, Victoria 3133 (AU). **EVANS, Stuart, Justin** [AU/AU]; 142 Bambra Road, Caulfield, Victoria 3162 (AU). **EVANS, Evan, Douglas** [AU/AU]; 6 Raphael Street, North Caulfield, Victoria 3161 (AU).

(74) Agent: **PHILLIPS ORMONDE & FITZPATRICK**; 367 Collins Street, Melbourne, Victoria 3000 (AU).

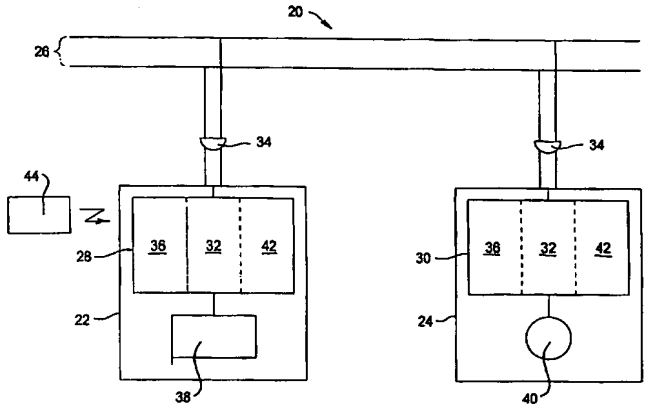
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: THEFT DETERRENCE SECURITY SYSTEM



(57) Abstract: A security system (20) for not enabling, enabling or disabling electrical devices for deterring theft, or preventing unauthorised use, of such devices. The security system comprises a plurality of electrical devices (22, 24) which are operationally linked via a bi-directional communication medium, which may be via a mains power supply (26) or a microwave or radiowave medium. Each electrical device includes a programmable means (28, 30) for controlling operation of the operative parts (38, 40) of the electrical devices. Each programmable means has a signal transmitting and receiving means (32) associated with it for transmitting and receiving control signals over the communication medium (26), with the programmable means (28) of one of the electrical devices (22) being programmed as a controller for the other electrical device(s) (24). Preferably the controller is provided via an electrical appliance which includes a data entry facility (44) for its programmable means (28) and the programmable means (28) is programmed both to operate the electrical appliance as such (42-38), and to provide the controller functions (36) for the security system (20). Various security functions for the security system are disclosed involving bi-directional communications between electrical devices which in the event of a security breach involving one device may result in all of the devices being rendered inoperative.

WO 2004/010395 A1

THEFT DETERRENCE SECURITY SYSTEM

Technical Field

The present invention relates to a security system for electrical devices for deterring theft of those devices. The invention is applicable, for example, to electrical devices for households, for example, appliances such as television sets, VCR or DVD players, radios, hi-fi systems, washing machines, microwave ovens, and the like. Generally, the invention is applicable to any electrical device that includes an operation controlling programmable means such as a microprocessor or PLD (programmable logic device).

A security system according to the invention may operate within a given environment (for example, a household or business) in respect of electrical devices that are connected to a mains (AC or DC) or other networked power supply system for that environment, wherein the power supply system provides a communication medium for the security system whereby control signals are transmitted/received via the mains power supply of an electrical device. However electrical devices that are otherwise powered, for example self-powered, and which can be operationally linked via a communication medium such as for example, a radio or microwave communication system, are also included within the scope of the invention. Such self-powered electrical devices include for example mobile (cellular) telephones, portable computers etc.

Background

International patent application publication number WO 02/11093 A1 discloses a theft deterrent system for mains powered appliances that incorporates a separate dedicated controller and one or more controlled appliances. The controller includes an automatic reset feature whereby, when left plugged in to the mains power supply, the controller will automatically transmit a reset signal to one or more appliances immediately after the mains power supply is restored to the controller following a mains power supply interruption. That is, operation of the reset feature occurs in the event of a mains power interruption and normal restoration thereof. For theft deterrence the appliance controller may include a motion sensing means and a battery

which will prevent the automatic re-setting of the appliances should the controller be moved whilst the mains power is disconnected.

A problem with this known theft deterrent system is that it is of limited versatility because all theft or non-theft events upon which a consequential system action occurs are wholly dependent upon the controller, that is, the system primarily operates via control signals transmitted from the controller and received by the protected appliance(s) in a master-slave relationship. Thus, for example, the automatic reset feature, the context for operation of which is interpreted as a non-theft event, requires a power interruption to the controller but without disconnection of the controller from the mains. When there is disconnection of the controller from the mains, which is interpreted as a theft event, the automatic reset feature is disabled.

An object of the present invention is to provide a security system (or methods of operation, or program products) for not enabling, enabling or disabling electrical devices (for example, household appliances) of the system for deterring theft of such devices, which is more versatile than the above described known system. The present invention includes various aspects (see below), which generally include a feature that a bi-directional communication protocol is followed before an electrical device protected by the system either remains inoperable, or is enabled or disabled. Another object is to provide an embodiment wherein all the electrical devices of the system will be disabled upon the detection of an unauthorised event in respect of only one of those devices.

The discussion herein of the background to the invention is included to explain the context of the invention. This is not to be taken as an admission that any of the material referred to was known or part of the common general knowledge in Australia as at the priority date of any of the claims of the present application.

Disclosure of the Invention

Most broadly, the invention is a security system for not enabling, enabling or disabling electrical devices for deterring theft of such devices which, equipment-wise, includes a plurality of electrical devices which are operationally linked via a bi-directional communication medium,

each electrical device including a programmable means for controlling operation of the electrical device,

each programmable means having a signal transmitting and receiving means associated therewith for transmitting and receiving control signals over the communication medium,

wherein the programmable means of one of the electrical devices is programmed as a controller for the other electrical devices.

The electrical device which includes the programmable means that provides the controller may be a dedicated controller as such, or alternatively it may be an electrical device such as an appliance which includes a data entry facility for its programmable means, and wherein its programmable means is programmed both to operate the electrical device or appliance as such and to provide the controller functions for the security system. In one broad form, the security system may involve only two electrical devices (for example, a dedicated controller and a household appliance or two household appliances one of which provides the controller functions for the other), however more usually the security system will involve several electrical devices. The equipment of the security system and its programming may also be such that if an existing controller is de-activated, another of the electrical devices of the system may be activated to provide the controller functions.

According to a first aspect of the invention the controller programmable means and the programmable means of the other electrical device or devices are programmed for a request-on control signal to be sent from an electrical device to the controller upon restoration of power to that electrical device following a power interruption thereto, and for the controller to return a turn-on control signal only if power to the controller has remained uninterrupted,

whereby that electrical device is enabled only if the controller has remained enabled.

This first aspect of the invention allows for an electrical device to be disconnected from and then re-connected to the security system without that occurrence being interpreted as an unauthorised or theft event. That is, that there has been no power outage at the controller is interpreted as the controller not having been tampered with. This, for example, allows an electrical appliance within a household to be re-located within that household and to automatically resume operation when power is reconnected. Of course, if the controller is not present or "on line" to receive the request-on control signal, the electrical device will not receive a return turn-on control signal and thus the electrical device will remain inoperable. Otherwise if there has been a power outage at the controller other consequences may follow. A preferable such consequence is that if an electrical device to which power is restored sends a request-on control signal to the controller and the controller does not recognise the requesting device, then the controller sends a turn-off control signal to all electrical devices on the system, whereby all the electrical devices of the system are disabled in the presence of one unauthorised electrical device.

Thus if, for example, an electrical device is stolen and is plugged into the thief's home having a similar security system, the electrical device will send out a request-on control signal to the controller and as a correctly coded controller will not be present, no turn-on control signal will be sent, thus the electrical device will remain inoperable. As a new electrical device is now on the thief's security system with a different security code (for example pin number), the thief's controller will deem stolen goods to be on the security system and send a global turn-off signal which then turns off all the appliances in the thief's house that have this security feature. All such devices will remain inoperable until an appropriate security code for that device is provided through the controller or the device is removed from the system and the local security code for the system is provided to the controller.

According to a second aspect of the invention, the controller programmable means and the programmable means of the other electrical device or devices are programmed for a roll-call control signal to be sent from the controller to the other electrical devices, and for the other electrical devices to respectively and in sequence return a 'present' control signal to the controller in response to receipt of the roll-call control signal. If a 'present' control signal is not returned by any electrical device, or is returned out of sequence, the controller will detect that a system change has occurred and commence a security check, for example a polling sequence as in the third aspect of the invention (which is described hereinbelow). This aspect of the invention allows for a security check of the whole security system to be implemented that keeps the control signals bandwidth to a minimum, which reduces possible interferences (noise) from the bi-directional communication medium. Preferably the controller is programmed for the roll-call control signal to be repeatedly randomly sent.

According to a third aspect of the invention, the controller programmable means and the programmable means of the other electrical device or devices are programmed for polling control signals to be sent from the controller to the other electrical devices upon restoration of power to the controller following a power interruption thereto, and for the other electrical devices to return request-on control signals to the controller in response to receipt of their respective polling control signals, and for the controller to then send turn-on control signals to the other electrical devices only if none of the other electrical devices are missing.

This third aspect of the invention also encompasses the controller programmable means and the programmable means of the other electrical device or devices being programmed for the polling control signals to be repeatedly sent from the controller to the other electrical devices. This feature provides an added level of security in that initiation of a security check of the whole security system is not dependent upon a power outage having occurred to the controller. The polling control signals may be repeatedly sent with random timing between each poll within a user defined maximum time window.

With the third aspect of the invention, if any of the electrical devices initially on the system are missing, the controller will not send a turn-on signal to the electrical devices. Thus changes to the security system by way of the absence of an initially present electrical device or the addition of an extra electrical device, possibly indicative of tampering with the system, for example re-location by a thief of all the electrical devices of a system including the controller to the thief's household and the thief seeking to activate some or all of the electrical devices within his own home which may include other electrical devices, will result in the stolen electrical devices not being enabled. Of course, if the changes to the security system are legitimate, a user merely needs to enter a security code into the controller to authorise the controller to turn-on the electrical devices.

Preferably with the third aspect of the invention, if an initially present device is missing, the controller sends turn-off control signals to all the electrical devices on the system whereby all the electrical devices of the system are disabled in the presence of one unauthorised electrical device or in the absence of a device that should be on the system.

Thus, in a theft situation for example where all the electrical appliances including the controller of a household are stolen and installed in another premises, the controller will immediately commence a poll by sending out polling control signals. If any other appliance having a similar security feature is detected, the controller will send out a global turn-off signal thereby disabling both the stolen and owned goods of the thief. Of course, if the changes to the security system are legitimate, a user merely needs to enter a security code into the controller to authorise the controller to turn-on the electrical devices.

Preferably, in any of the above aspects of the invention, the controller programmable means is programmed to send turn-off control signals to all the electrical devices after a predetermined period (hereinafter termed an automatic "time out" feature) unless a security code is entered into the controller prior to the end of the predetermined period. Thus, for example, in a situation where a thief steals all the electrical devices and the controller of a household and plugs

them all into the mains power system at a different premises, and there are no additional security protected electrical devices in that premises, then the electrical appliances will initially be enabled (see the third aspect of the invention), but will then be disabled after a time period in the absence of the thief entering a correct security code into the controller.

The above preferred feature is suitable, for example, for use in the rental market wherein an appliance may be accorded a security code that lasts for a predetermined period of time and the appliance will be disabled after that time period unless another security code is set via a controller for the appliance.

According to a fourth aspect of the invention, a security system having various of the features as described above may be realised in respect of a single electrical device, wherein the electrical device includes a programmable means for controlling operation of the electrical device, and that programmable means is also programmed as a security controller for the electrical device. Thus, according to this aspect of the invention, an electrical device can act as its own security controller. Most preferably in this aspect of the invention, the programmable means is programmed for a turn-off control signal to be generated after a predetermined period unless a security code is entered into the controller prior to the end of the predetermined period.

This fourth aspect of the invention primarily serves as security for the rental market wherein the electrical device may be accorded a security code that lasts for a predetermined period of time (for example, the intended rental duration) and the electrical device will be disabled after that time period unless that or another security code (as may be appropriate) is entered into the controller portion of the programmable means.

Another preferred feature in relation to any of the above aspects of the invention is for the controller programmable means to be programmed to randomly, within a user defined maximum time window, send a stay-on control signal to at least one of the electrical devices, and for that electrical device to be programmed to turn-off if the stay-on signal is not received.

The roll-call or polling control signals of the second and third aspects of the invention and the stay-on control signal of the immediately preceding preferred feature may be randomly timed within a user defined maximum time window. This has an added security advantage in that there is no consistency in the signal timing over the communication medium thus rendering such signalling difficult to monitor or replicate by a would-be thief.

A further preferred feature is that the programming is such that whenever the operational status of an electrical device of the system is changed, for example an appliance is switched from a "standby" mode to "on", that change is communicated to the controller. Thus the controller may monitor not only the presence of electrical devices, but also their current operational statuses.

A security system according to the invention in its various aspects may also be part of a monitored security alarm system wherein the monitoring is typically at a remote centralised security concern or police station. Thus, for example, based on the roll-call operational scenario (the second aspect of the invention), if thieves are removing electrical devices from the security system in a monitored premises, this will be evident at the remote monitoring station in real time and security personnel can be despatched to the monitored premises and be forewarned about which devices have been removed from the security system.

The programming of the programmable means of the electrical device or devices of a security system according to the invention may be encrypted as known in the art for added security. Alternatively such encryption may be specifically developed for the present invention.

In the case of a security system according to the invention in its various aspects being based on a mains power supply system, the electrical device or devices of the system will not require its or their own respective dedicated power supplies, that is, all necessary power for both the normal operation of an electrical device and for its operation in the security system is supplied from the

mains. However a security system according to the invention may operate in respect of electrical devices that include their own dedicated power supplies, for example, from a battery or batteries incorporated in each device, so long as a suitable communication medium (for example, radio or microwaves) operationally links the electrical devices to the system. The invention also includes a security system wherein one or some of the electrical devices thereof may be mains powered and another or others of the electrical devices may have their own internal power supply.

A security system according to the system may also have added versatility in that the programming can be such as to configure a given electrical device to be recognised by more than one controller, or a given controller can be configured to recognise a number of different security codes.

Another optional feature is that the programming can be such that the controller of a security system may be used to program the operation of one or more of the other electrical devices of the system. Thus for example, the system controller may be used to program a VCR to record a selected TV show whilst a home occupant is absent, or to switch on an air-conditioning unit at a selected time prior to the arrival of a house occupant.

An electrical device of a security system according to the invention may also be programmed for it to be automatically disabled after a predetermined time period, unless a security code is inputted. A predetermined time period may be several days such as for example will allow the electrical device to be sent to a repair shop for repairs.

Persons skilled in this art will appreciate that all of the above aspects of the invention, including its various preferred or optional features, which are described as embodied via hardware (that is, equipment) may alternatively or additionally be realised via methods of operation involving a plurality of electrical devices, or as program products for programming the electrical devices.

For a better understanding of the invention and to show how it may be carried into effect, an example thereof will now be described, by way of non-limiting example only, with reference to the accompanying drawings.

Brief Description of the Drawings

Fig.1 schematically illustrates the equipment of a security system according to an embodiment of the invention.

Figs 2 to 5 are flow charts that show programming and operating sequences for electrical devices of a security system according to embodiments of the invention.

Detailed Description

A security system 20 (see Fig. 1) according to an embodiment of the invention includes a plurality of electrical devices 22, 24 which are operationally linked via a bi-directional communication medium, in this embodiment an a.c. mains power supply 26. Each electrical device 22, 24 includes a programmable means, respectively 28, 30, each of which includes a signal transmitting and receiving means 32 for transmitting and receiving control signals over the communication medium (mains) 26. Each electrical device 28, 30 is connected to the mains 26 via a plug and socket 34, as is well known. The respective programmable means 28, 30 of the electrical devices 22, 24 are programmed (or programmable) for operation in the security system (schematically illustrated as part 36) and to operate the particular controlled components 38, 40 of the respective electrical devices 22, 24 (schematically illustrated as part 42). In the illustrated security system 20, electrical device 22 includes a data entry facility 44 for entering data into its programmable means 28. Facility 44 may be a key board that is hard wired to the electrical device 22 (for example as in a computer), or a remote device (for example as in a remote control device for a TV or VCR or DVD player). In the security system 20, electrical device 22 is programmed (or programmable) as a controller for the other electrical device 24 because it has data entry facility 44. The security system 20 may include more than two electrical devices for which the electrical device 22 is the controller.

Typically each electrical device 22, 24, etc will have an LCD device operationally linked to its programmable means 28, 30, etc for displaying messages associated with the operation of the security system, such as for example requesting entry of a security code (pin number), or a warning about an unauthorised system or electrical device status, or a normal system or electrical device status.

The programmable means 28 or 30 of the electrical devices 22, 24 may be an AMDEL Model No. AT 89C4051 microprocessor, or other microprocessor that is suitable for programming according to the requirements of the invention.

Fig. 2 is a flow chart (Flow Chart 1) that illustrates a sequence of possible events which can occur when an electrical device that has been programmed to be a controlled device 24 in a theft deterrence security system 20 herein described, is powered up in an environment where a programmed security controller 22 is installed and on-line. This flow chart illustrates a system where the controller uses a "roll call" technique to monitor devices on the system.

Immediately after power is applied to the device (Box 1), it waits for a pre-determined time interval (Box 2) to allow time for the receipt of a "roll call" or polling request from the controller (as in the second or third aspects of the invention). Such a request will occur if the controller was powered up at the same time as the device was powered up, eg. on restoration of mains power following a power failure. Although the device is powered up, it is not enabled at this point and will not work, but is capable of receiving and transmitting signals relating to security functions.

If a "roll call" request is received, (Box 3, YES response) the device transmits a response to the controller within a predefined time slot relative to the receipt of the request (Box 4). If the controller interprets the response as being valid according to its programmed criteria (Box 5 YES response, the controller transmits a "turn on" instruction to the device. The device is thereby enabled and will operate normally (Box 6). If the controller did not interpret the response

from the device as valid (Box 5 NO response), it will transmit a global "turn off" instruction to all devices on the system, which then cease operation (Box 16).

If a "roll call" request was not received during the waiting period (Box 3 NO response), the device transmits a "request on" signal to the controller (Box 7) (as in the first aspect of the invention). This signal includes information which identifies the device, including its security code. If the controller recognises the device as one which belongs to this system, or which belongs to another system but is allowed to be on this system as a "guest" (Box 8 YES response), it will transmit a "turn on" instruction to the device (Box 6).

If the controller did not recognise the device (Box 8 NO response), the controller issues a warning of an unauthorised device on the system and requests that a security code for the device be provided or that the device be disconnected from the system (Box 9). If the system owner knows the security code for the device (Box 10 YES response) and wishes to log the device onto the system as a "guest" (Box 11 YES response), the owner must enter both the device security code and the system security code on the controller (Box 12). The controller then transmits a "turn on" instruction to the "guest" device, which is thereby enabled and operates normally.

If the system owner does not know the device security code (Box 10 NO response) or does not want to log the device onto the system as a "guest" (Box 11 NO response), the unauthorised device must be disconnected from the system (Box 14). If disconnection occurs within a pre-determined time period (Box 15 YES response) no further action occurs and the system operates normally.

If the unauthorised device was not disconnected within the allowable time period (Box 15 NO response), the controller transmits a global "turn off" instruction to all devices on the system, which then cease operation (Box 16). If the system owner then wishes to re-enable all devices on the system (Box 17 YES response), this is possible at any time by disconnecting the unauthorised device and entering the system security code (Box 18).

Fig. 3 is a flow chart (Flow Chart 2) that illustrates a sequence of possible events which can occur when an electrical device that has been programmed to be a controller 22 of a theft deterrence security system 20 herein described is powered up and remains on-line, in an environment where it is monitoring and controlling the security functions of other programmed devices 24. This flow chart illustrates a system where the controller uses a "roll call" technique to monitor devices on the system.

Immediately after power is applied to the programmed controller (Box 1) it transmits a global "roll call" request to all devices on the system, and waits for a response from each device in a defined sequence according to its address on the system (Box 2) (as in the second aspect of the invention).

If no devices that are logged onto the system failed to respond (Box 3 NO response) and no replies were received in an incorrect sequence, or from devices not logged onto the system (Box 4 NO response) the controller deems that there is no abnormality on the system (Box 5 NO response). If the "roll call" request was preceded by a power failure at the controller (Box 6 YES response) the controller then transmits a global "turn on" instruction to all devices (Box 7) since it can be assumed that the power failure had also shut down the other devices on the system and they will need to be turned on again. If the "roll call" request was not preceded by a power failure, but was one of the routine requests that occur at random time intervals (as preferred in the second aspect of the invention) (Box 6 NO response) no "turn on" instruction is transmitted, so as to avoid unnecessary signalling on the communications medium. In either case, after a random time delay (Box 8) a new "roll call" will be initiated (Box 2).

If any device that was logged on to the system at the previous roll call failed to respond (Box 3 YES response), the controller checks whether the missing device is either a "transistory" device or a "guest device". (A transistory device is one which has been programmed as such, and can be removed from the system and brought back without requiring any log off or log on action. A

"guest" device is one which is part of another security system but the present system has been programmed to accept it, typically for a limited time period).

If the missing device is either transistory or guest (Box 9 YES response), the controller checks whether a reply was received in incorrect sequence or from any device not logged onto the system. If a response is received in an incorrect sequence or from a device that is not logged onto the system (Box 4 YES response) and the unlogged device is either transistory or a guest (Box 11 YES response), the system also deems that there is no abnormality on the system (Box 5 NO response).

If a missing device is not transistory or guest (Box 9 NO response), the controller issues a warning of a device missing from the system (Box 10). Similarly, if a device that is not logged on is not transistory or guest (Box 11 NO response) or a reply was received in an incorrect sequence, the controller issues a warning of unauthorised devices on the system (Box 12). If either or both warnings are issued, an abnormality exists on the system (Box 5 YES response) and the controller requests that the security code be entered (Box 13) and the abnormality be addressed within a predetermined time limit by logging in or disconnecting unauthorised devices, or by logging out or reconnecting missing devices. If the appropriate action is not taken within the allowable time limit (Box 14 NO response), the controller transmits a global "turn off" instruction to all devices on the system (Box 15). The controller then repeats the request for the security code (Box 15), and the cycle repeats until the abnormality is corrected.

The system also has an automatic "time out" feature which is initiated at owner defined intervals if the security code has not been entered at any time within this interval. When the "time out" limit is approaching, the controller issues an audible and visual warning accompanied by a request for the security code for a predetermined time (Box 16). If the security code is not entered before the time out limit has been reached (Box 17 NO response) the controller transmits a global "turn off" instruction to all devices on the system. If the security code was entered before the time out limit was reached (Box 17 YES

response) the time out timer is reset to zero and the timing sequence recommences (Box 18). This timer is reset to zero at any other time the security code is entered, for example Box 14 YES response.

Fig 4 (Flow Chart 3) illustrates a sequence of possible events which can occur when an electrical device that has been programmed to be a controlled device 24 in a theft deterrence security system 20 herein described, is powered up in an environment where a programmed security controller 22 is installed and on-line. This flow chart illustrates a system where the controller uses a polling technique to monitor devices on the system as in the third aspect of the invention.

Immediately after power is applied to the device (Box 1), it waits for a pre-determined time interval (Box 2) to allow time for the receipt of polling request from the controller. Such a request will occur if the controller was powered up at the same time as the device was powered up, eg. on restoration of mains power following a power failure. Although the device is powered up, it is not enabled at this point and will not work, but is capable of receiving and transmitting signals relating to security functions.

If a polling request is received, (Box 3, YES response) the device transmits its pre-programmed response to the controller (Box 4). If the controller interprets the response as being valid according to its programmed criteria (Box 5 YES response), the controller transmits a "turn on" instruction to the device. The device is thereby enabled and will operate normally (Box 6). If the controller did not receive the response from the device or did not interpret it as valid (Box 5 NO response), it will transmit a global "turn off" instruction to all devices on the system, which then cease operation (Box 16).

If a polling request was not received during the waiting period (Box 3 NO response), the device transmits a "request on" signal to the controller (Box 7). This signal includes information which identifies the device, including its security code. If the controller recognises the device as one which belongs to this system, or which belongs to another system but is allowed to be on this system

as a "guest" (Box 8 YES response), it will transmit a "turn on" instruction to the device (Box 6).

If the controller did not recognise the device (Box 8 NO response), the controller issues a warning of an unauthorised device on the system and requests that a security code for the device be provided or that the device be disconnected from the system (Box 9). If the system owner knows the security code for the device (Box 10 YES response) and wishes to log the device onto the system as a "guest" (Box 11 YES response), the owner must enter both the device security code and the system security code on the controller (Box 12). The controller then transmits a "turn on" instruction to the "guest" device, which is thereby enabled and operates normally.

If the system owner does not know the device security code (Box 10 NO response) or does not want to log the device onto the system as a "guest" (Box 11 NO response), the unauthorised device must be disconnected from the system (Box 14). If disconnection occurs within a pre-determined time period (Box 15 YES response) no further action occurs and the system operates normally.

If the unauthorised device was not disconnected within the allowable time period (Box 15 NO response), the controller transmits a global "turn off" instruction to all devices on the system, which then cease operation (Box 16). If the system owner then wishes to re-enable all devices on the system (Box 17 YES response), this is possible at any time by disconnecting the unauthorised device and entering the system security code (Box 18).

Fig. 5 (Flow Chart 4) illustrates a sequence of possible events which can occur when an electrical device 22 that has been programmed to be a controller of the theft deterrence security system 20 is powered up and remains on-line, in an environment where it is monitoring and controlling the security functions of other programmed devices. This flow chart illustrates a system where the controller uses a polling technique to monitor devices on the system.

Immediately after power is applied to the programmed controller (Box 1) it transmits polling requests in turn to each device on the system, and waits for a defined time for a response from the polled device before polling the next device (Box 2).

If no devices that are logged onto the system failed to respond (Box 3 NO response) and if the polling request was preceded by a power failure at the controller (Box 4 YES response) the controller then transmits a global "turn on" instruction to all devices (Box 5) since it can be assumed that the power failure had also shut down the other devices on the system, and they will need to be turned on again. If the polling request was not preceded by a power failure, but was one of the routine requests that occur at random time intervals (Box 4 NO response) no "turn on" instruction is transmitted, so as to avoid unnecessary signalling on the communications medium. In either case, after a random time delay (Box 6) a new polling request will be initiated (Box 2).

If any device that was logged on to the system at the previous poll failed to respond (Box 3 YES response), the controller checks whether the missing device is either a "transitory" device or a "guest device". (A transitory device is one which has been programmed as such, and can be removed from the system and brought back without requiring any log off or log on action. A "guest" device is one which is part of another security system but the present system has been programmed to accept it, typically for a limited time period.)

If the missing device is either transitory or guest ((Box 7 YES response), the controller checks whether the polling request was preceded by a power failure (Box 4) and proceeds accordingly.

If a missing device is not transitory or guest (Box 7 NO response), the controller issues a warning of a device missing from the system (Box 8) and identifies the missing device(s). The controller then makes a request for the security code to be entered and for the abnormality to be addressed (Box 9). If the missing device is not logged out or reconnected within the allowable time limit (Box 10 NO response), the controller transmits a global "turn off" instruction

to all devices on the system (Box 11). The controller then repeats the request for the security code (Box 9), and the cycle repeats until the abnormality is corrected.

The system also has an automatic "time out" feature which is initiated at owner defined intervals if the security code has not been entered at any time within this interval. When the "time out" limit is approaching, the controller issues an audible and visual warning accompanied by a request for the security code for a predetermined time (Box 12). If the security code is not entered before the time out limit has been reached (Box 13 NO response) the controller transmits a global "turn off" instruction to all devices on the system. If the security code was entered before the time out limit was reached (Box 13 YES response) the time out timer is reset to zero (Box 14) and the timing sequence recommences. This timer is also reset to zero at any other time the security code is entered, for example Box 10 YES response.

The invention described herein is susceptible to variations, modifications and/or additions other than those specifically described and it is to be understood that the invention includes all such variations, modifications and/or additions which fall within the scope of the following claims.

CLAIMS:

1. A security system for not enabling, enabling or disabling electrical devices for deterring theft, or preventing unauthorised use, of such devices including a plurality of electrical devices which are operationally linked via a bi-directional communication medium,

each electrical device including a programmable means for controlling operation of the electrical device,

each programmable means having a signal transmitting and receiving means associated therewith for transmitting and receiving control signals over the communication medium,

wherein the programmable means of one of the electrical devices is programmed as a controller for the other electrical devices.

2. A security system as claimed in claim 1 wherein the electrical device which includes the programmable means that provides the controller is an electrical appliance which includes a data entry facility for its programmable means, and wherein its programmable means is programmed both to operate the electrical appliance as such and to provide the controller functions for the security system.

3. A security system as claimed in claim 1 or 2 wherein the controller programmable means and the programmable means of the other electrical device or devices are programmed for a request-on control signal to be sent from an electrical device to the controller upon restoration of power to that electrical device following a power interruption thereto, and for the controller to return a turn-on control signal only if power to the controller has remained uninterrupted, whereby that electrical device is enabled only if the controller has remained enabled.

4. A security system as claimed in claim 3, wherein if an electrical device to which power is restored sends a request-on control signal to the controller and the controller does not recognise the requesting device, then the controller sends a turn-off control signal to all electrical devices on the system, whereby

all the electrical devices of the system are disabled in the presence of one unauthorised electrical device.

5. A security system as claimed in claim 4 wherein all the electrical devices remain inoperable until an appropriate security code for that unauthorised device is provided through the controller or the unauthorised device is removed from the system and a local security code for the system is provided to the controller.

6. A security system as claimed in claim 1 or 2 wherein the controller programmable means and the programmable means of the other electrical device or devices are programmed for a roll-call control signal to be sent from the controller to the other electrical devices, and for the other electrical devices to respectively and in sequence return a 'present' control signal to the controller in response to receipt of the roll-call control signal.

7. A security system as claimed in claim 6 wherein if a 'present' control signal is not returned by any electrical device, or is returned out of sequence, the controller will detect that a system change has occurred and commence a security check.

8. A security system as claimed in claim 1 or 2 wherein the controller programmable means and the programmable means of the other electrical device or devices are programmed for polling control signals to be sent from the controller to the other electrical devices upon restoration of power to the controller following a power interruption thereto, and for the other electrical devices to return request-on control signals to the controller in response to receipt of their respective polling control signals, and for the controller to then send turn-on control signals to the other electrical devices only if none of the other electrical devices are missing.

9. A security system as claimed in claim 8 wherein the controller programmable means and the programmable means of the other electrical

device or devices are programmed for the polling control signals to be repeatedly sent from the controller to the other electrical devices.

10. A security system as claimed in claim 9 wherein polling control signals are repeatedly sent with random timing between each poll within a user defined maximum time window.

11. A security system as claimed in any one of claims 8 to 10 wherein if an initially present device is missing, the controller sends turn-off control signals to all the electrical devices on the system whereby all the electrical devices of the system are disabled in the presence of one unauthorised electrical device or in the absence of a device that should be on the system.

12. A security system as claimed in any one of claims 1 to 11 wherein the controller programmable means is programmed to send turn-off control signals to all the electrical devices after a predetermined period unless a security code is entered into the controller prior to the end of the predetermined period.

13. A security system for not enabling, enabling or disabling an electrical device for deterring theft, or preventing unauthorised use, of that device, wherein the electrical device includes a programmable means for controlling operation of the electrical device as such, and a data input facility associated with the programmable means, and wherein that programmable means is also programmed as a security controller for the electrical device.

14. A security system as claimed in claim 13 wherein the programmable means is programmed for a turn-off control signal to be generated after a predetermined period unless a security code is entered into the controller prior to the end of the predetermined period.

15. A security system as claimed in any one of claims 1 to 14 wherein the controller programmable means is programmed to randomly, within a user defined maximum time window, send a stay-on control signal to at least one of

the electrical devices, and for that electrical device to be programmed to turn-off if the stay-on signal is not received.

16. A security system as claimed in claim 15 wherein the stay-on control signal is randomly timed within a user defined maximum time window.

17. A security system as claimed in any one of claims 1 to 16 wherein the programming is such that whenever the operational status of an electrical device of the system is changed (for example an appliance is switched from a "standby" mode to "on") that change is communicated to the controller whereby the controller monitors not only the presence of electrical devices, but also their current operational statuses.

18. A security system as claimed in any one of claims 1 to 17 wherein the security system is based on a mains power supply system, whereby all necessary power for both the normal operation of an electrical device and for its operation in the security system is supplied from the mains, and whereby the mains power supply system is used as the bi-directional communication medium.

19. A security system as claimed in any one of claims 1 to 17 wherein the security system involves electrical devices that include their own dedicated power supplies (for example, from a battery or batteries incorporated in each device), and a wireless communication medium (for example, radio or microwaves) operationally links the electrical devices to the system.

20. A security system as claimed in any one of claims 1 to 19 wherein the security system is interfaced with a general alarm system, and is capable of transmitting alarm or other signals to the general alarm system, and receiving control signals from the general alarm system.

21. A security system as claimed in any one of claims 1 to 19 wherein the controller for the security system is a controller associated with a general alarm system, and the controller includes programmable means programmed both to

operate the general alarm system and to provide the controller functions for the security system.

22. A security system as claimed in any of claims 1 to 21 wherein the system is programmed to allow any of the electrical devices, other than the controller, to operate as 'transitory' devices wherein they may be removed from, and returned to, the security system without creating a security breach or system abnormality, and wherein said 'transitory' devices are programmable to also operate in other compatible security systems.

23. A security system as claimed in any of claims 1 to 22 wherein the system is programmed to allow compatible electrical devices that are not part of the system, to operate as 'guest' devices on the system for a defined period of time, without creating a security breach or system abnormality.

24. A security system as claimed in any of claims 1 to 23 wherein any of the electrical devices, other than the controller, is programmable via the controller to operate for a defined period of time in an environment where there is either no security system, or there is a security system in which the device is not programmed as either a 'transitory' device or a 'guest' device.

25. A security system as claimed in any one of claims 1 to 24 wherein the system is programmed for the controller to program the operation of one or more of the other electrical devices of the system.

26. A computer program for a security system, the computer program providing for operation of the security system as claimed in any one of claims 1 to 25.

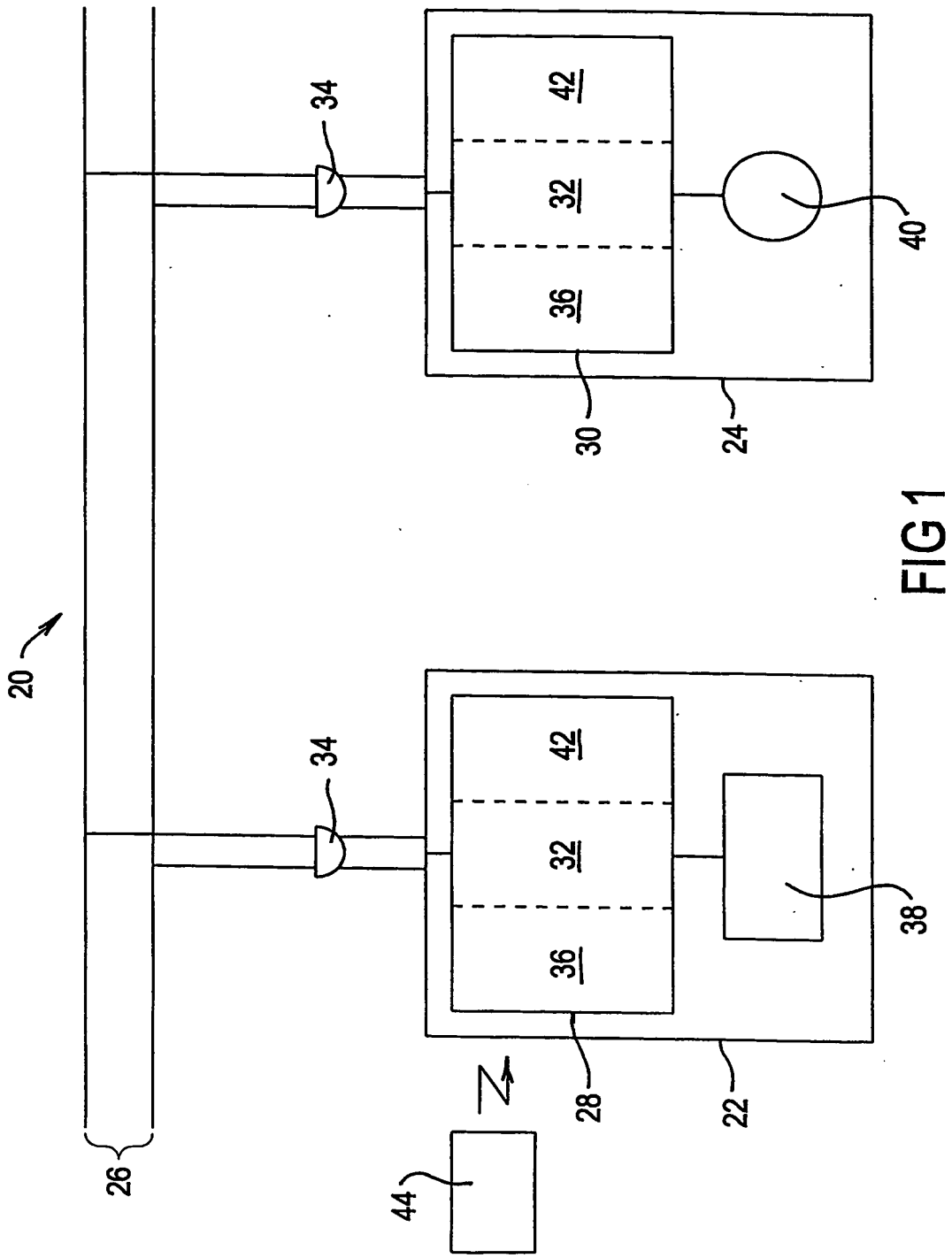


FIG 1

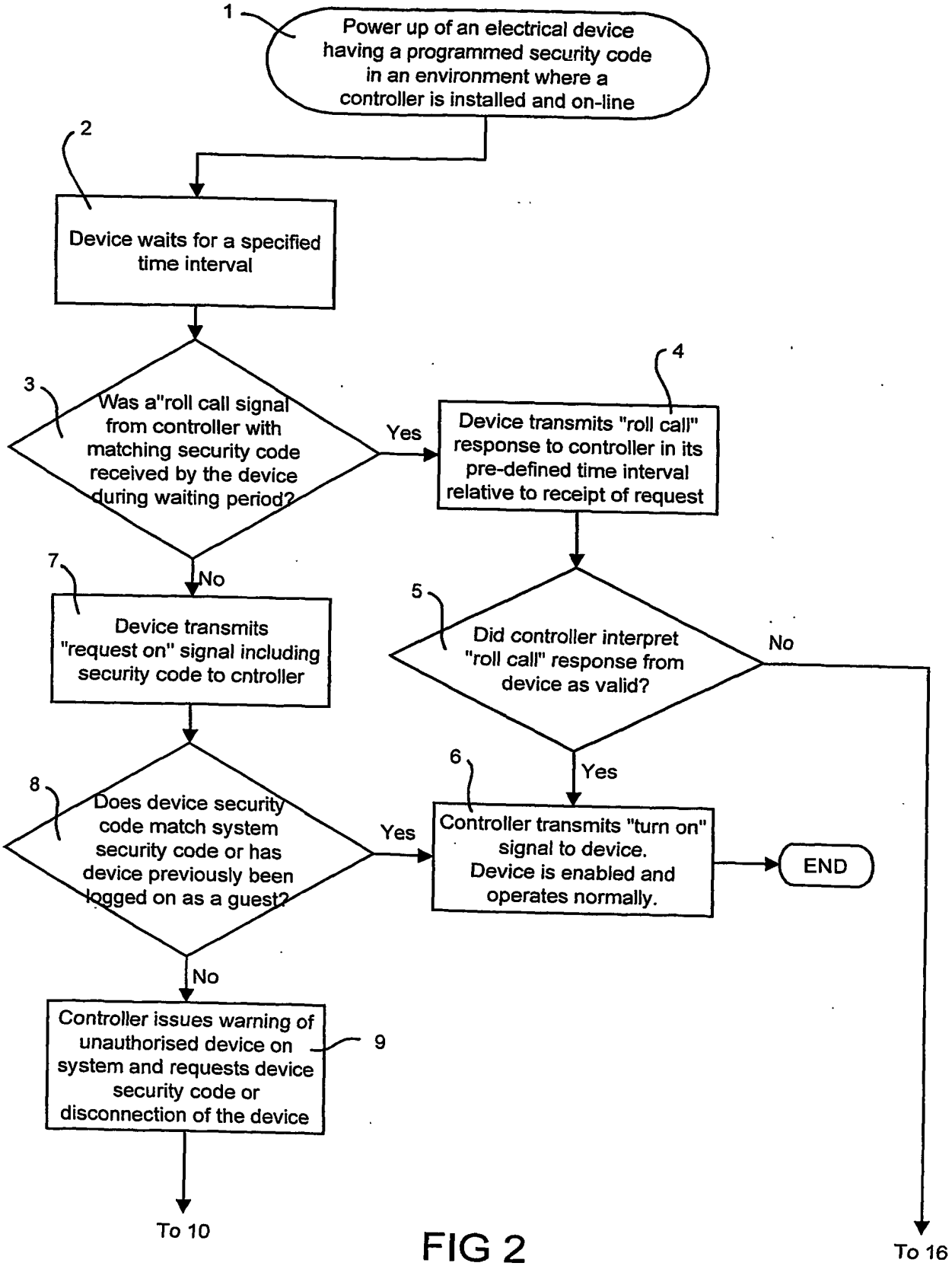
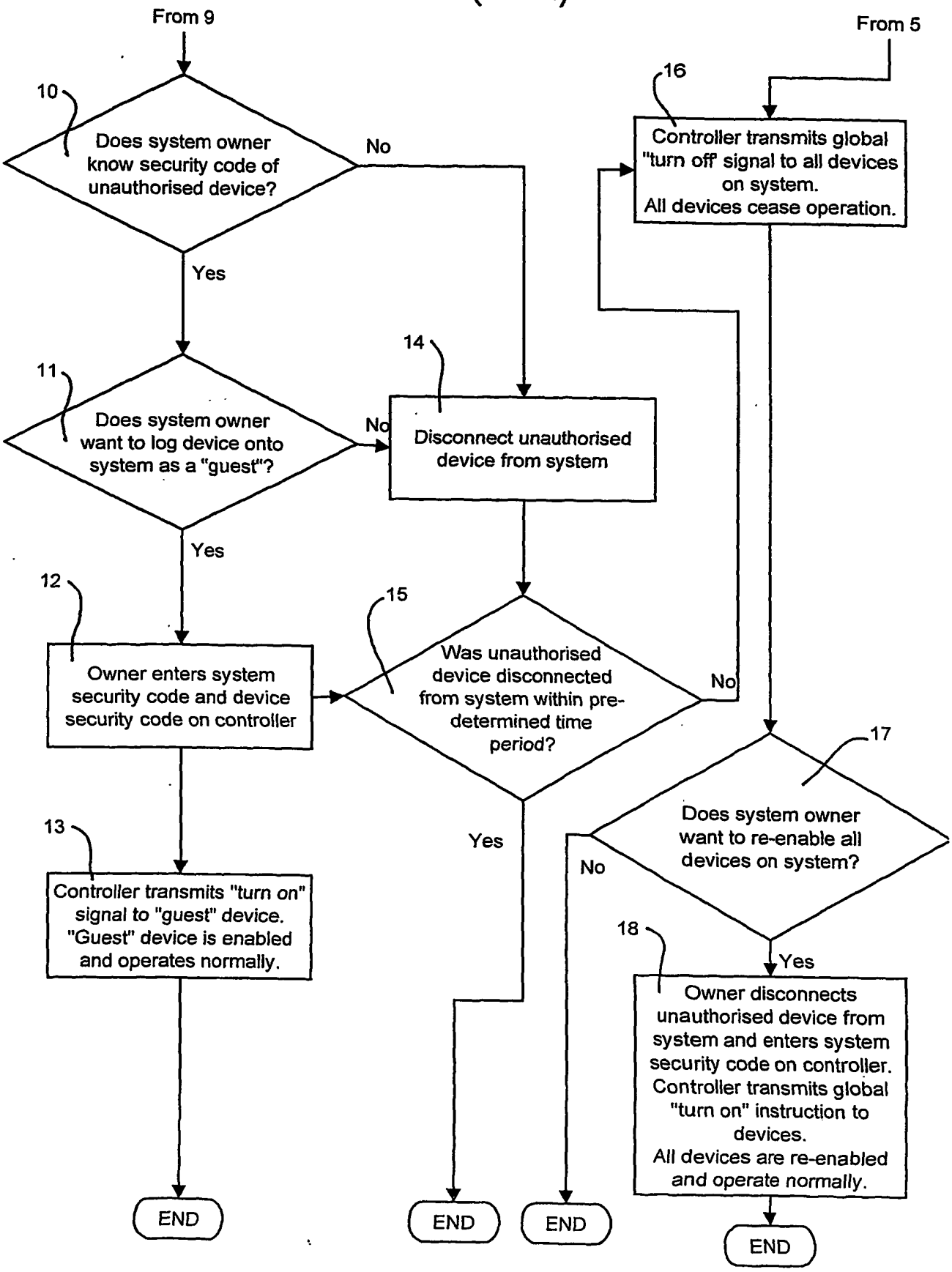

1
Power up of an electrical device having a programmed security code in an environment where a controller is installed and on-line
2
Device waits for a specified time interval
3
Was a"roll call signal from controller with matching security code received by the device during waiting period?
Yes
4
Device transmits "roll call" response to controller in its pre-defined time interval relative to receipt of request
5
Did controller interpret "roll call" response from device as valid?
No
To 16
Yes
6
Controller transmits "turn on" signal to device. Device is enabled and operates normally.
END
No
7
Device transmits "request on" signal including security code to cntroller
8
Does device security code match system security code or has device previously been logged on as a guest?
Yes
No
9
Controller issues warning of unauthorised device on system and requests device security code or disconnection of the device
To 10

FIG 2

FIG 2 (cont)


From 9
From 5
10
Does system owner know security code of unauthorised device?
No
Yes
11
Does system owner want to log device onto system as a "guest"?
No
Yes
14
Disconnect unauthorised device from system
12
Owner enters system security code and device security code on controller
15
Was unauthorised device disconnected from system within pre-determined time period?
No
Yes
16
Controller transmits global "turn off" signal to all devices on system.
All devices cease operation.
17
Does system owner want to re-enable all devices on system?
No
Yes
18
Owner disconnects unauthorised device from system and enters system security code on controller.
Controller transmits global "turn on" instruction to devices.
All devices are re-enabled and operate normally.
13
Controller transmits "turn on" signal to "guest" device.
"Guest" device is enabled and operates normally.
END
END
END
END

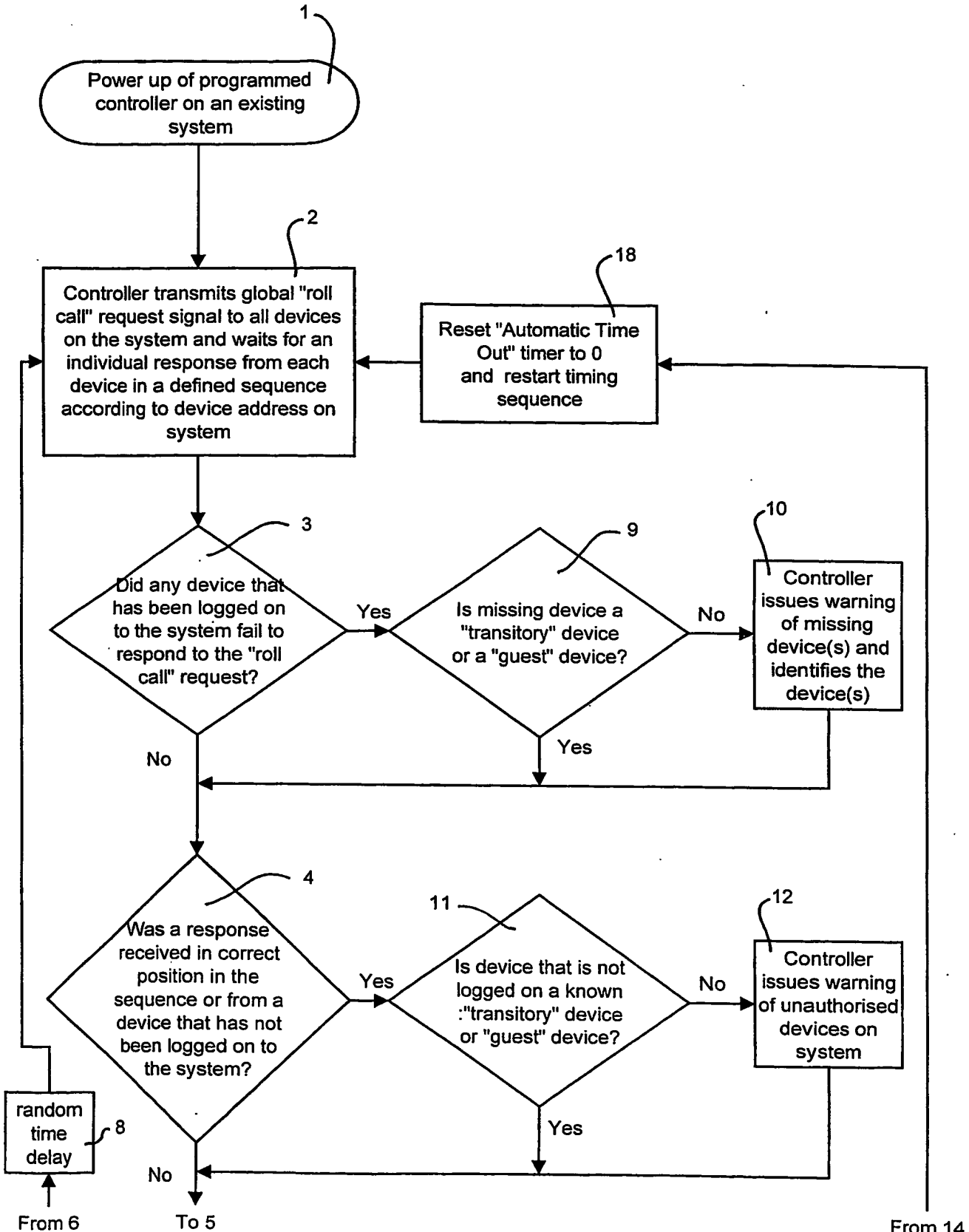

1
Power up of programmed controller on an existing system
2
Controller transmits global "roll call" request signal to all devices on the system and waits for an individual response from each device in a defined sequence according to device address on system
18
Reset "Automatic Time Out" timer to 0 and restart timing sequence
3
Did any device that has been logged on to the system fail to respond to the "roll call" request?
Yes
9
Is missing device a "transitory" device or a "guest" device?
No
10
Controller issues warning of missing device(s) and identifies the device(s)
Yes
No
4
Was a response received in correct position in the sequence or from a device that has not been logged on to the system?
Yes
11
Is device that is not logged on a known :"transitory" device or "guest" device?
No
12
Controller issues warning of unauthorised devices on system
Yes
No
random time delay
8
From 6
To 5
From 14

FIG 3

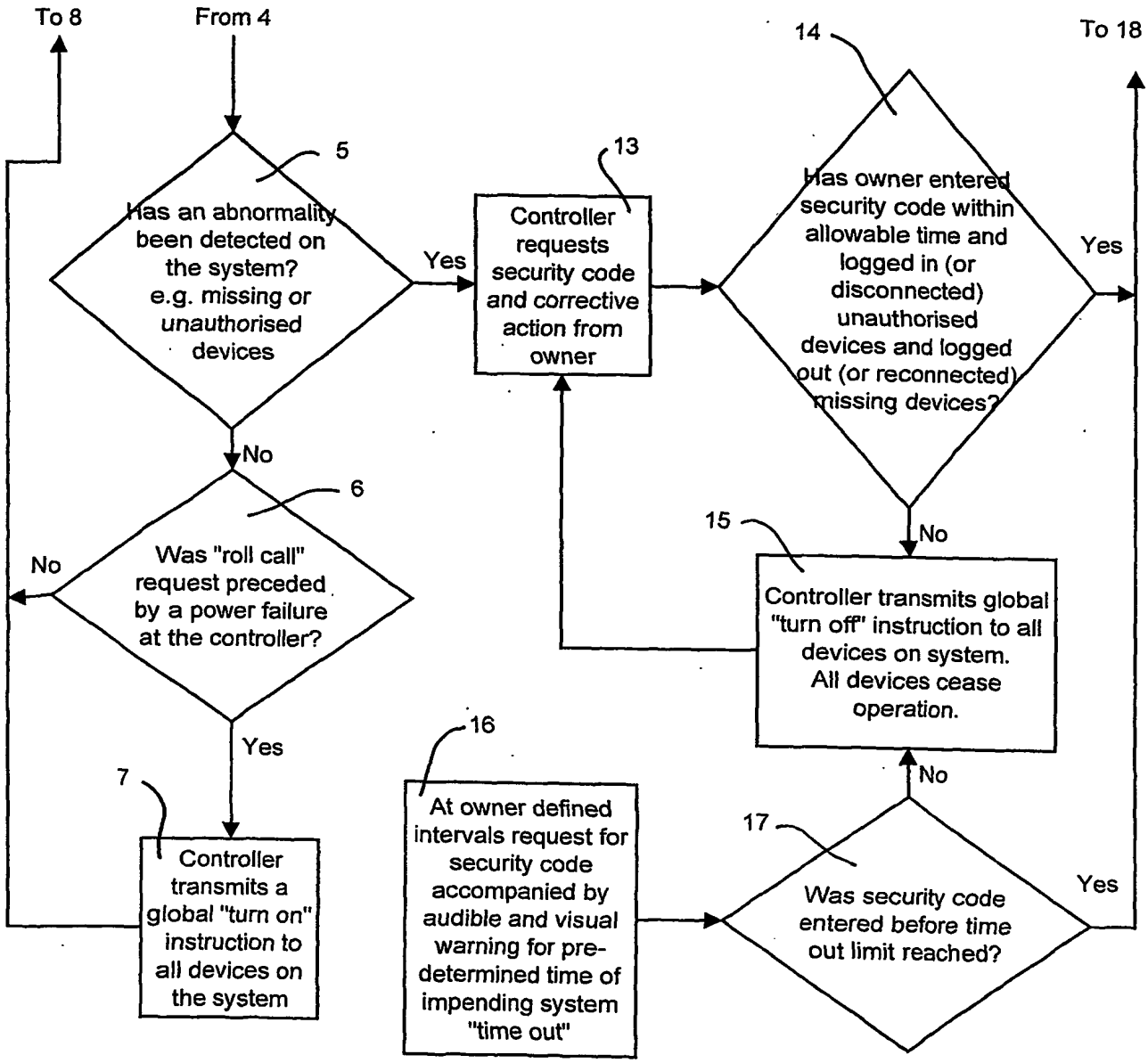

To 8
From 4
5
Has an abnormality been detected on the system? e.g. missing or unauthorised devices
Yes
13
Controller requests security code and corrective action from owner
14
Has owner entered security code within allowable time and logged in (or disconnected) unauthorised devices and logged out (or reconnected) missing devices?
Yes
To 18
No
6
Was "roll call" request preceded by a power failure at the controller?
No
Yes
15
Controller transmits global "turn off" instruction to all devices on system. All devices cease operation.
7
Controller transmits a global "turn on" instruction to all devices on the system
16
At owner defined intervals request for security code accompanied by audible and visual warning for pre-determined time of impending system "time out"
17
Was security code entered before time out limit reached?
No
Yes

FIG 3 (cont)

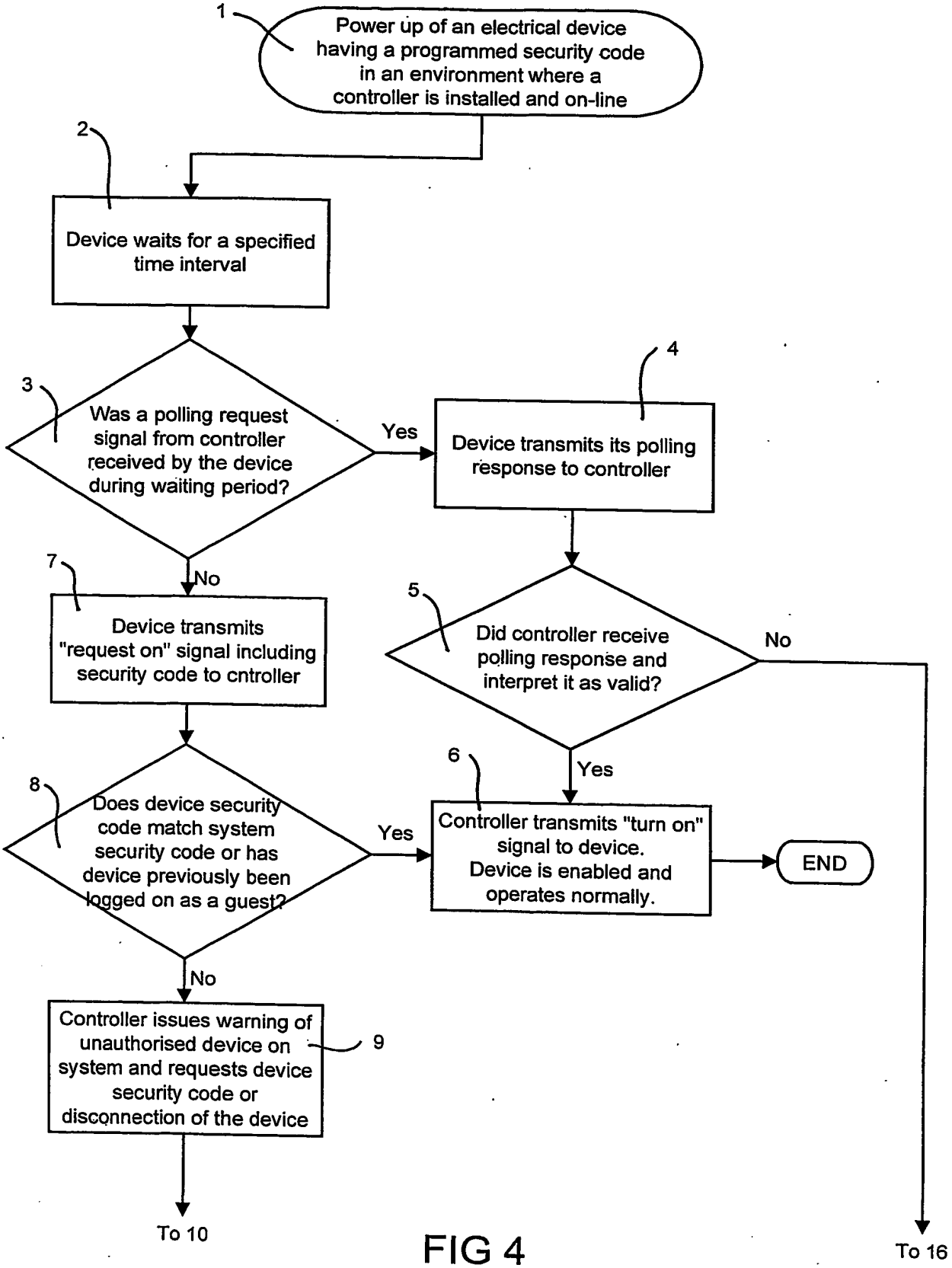
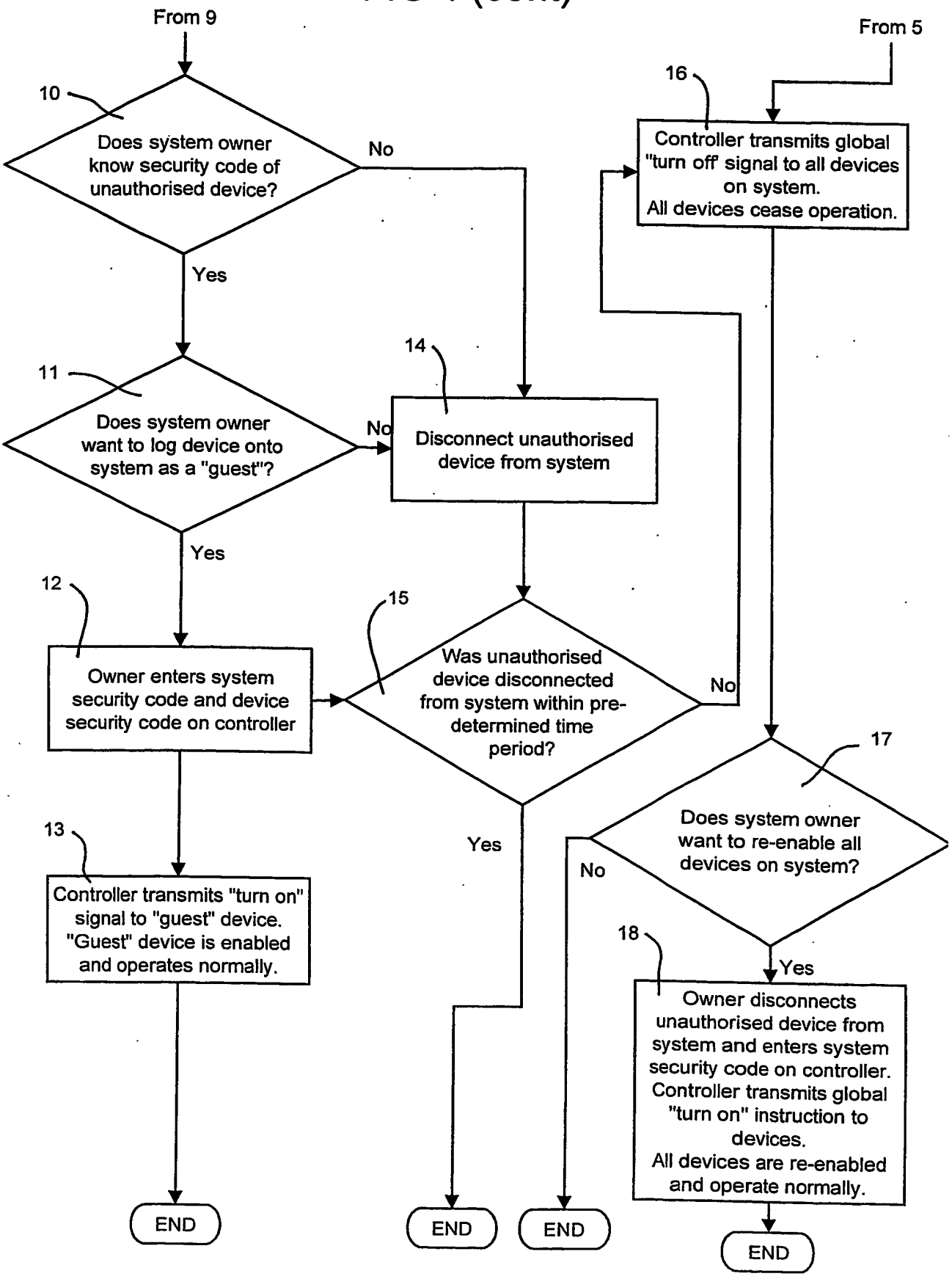

1
Power up of an electrical device having a programmed security code in an environment where a controller is installed and on-line
2
Device waits for a specified time interval
3
Was a polling request signal from controller received by the device during waiting period?
Yes
4
Device transmits its polling response to controller
No
7
Device transmits "request on" signal including security code to cntroller
5
Did controller receive polling response and interpret it as valid?
No
Yes
6
8
Does device security code match system security code or has device previously been logged on as a guest?
Yes
Controller transmits "turn on" signal to device. Device is enabled and operates normally.
END
No
Controller issues warning of unauthorised device on system and requests device security code or disconnection of the device
9
To 10
To 16

FIG 4

FIG 4 (cont)


From 9
10
Does system owner know security code of unauthorised device?
No
Yes
11
Does system owner want to log device onto system as a "guest"?
No
Yes
12
Owner enters system security code and device security code on controller
13
Controller transmits "turn on" signal to "guest" device. "Guest" device is enabled and operates normally.
END
14
Disconnect unauthorised device from system
15
Was unauthorised device disconnected from system within pre-determined time period?
No
Yes
END
From 5
16
Controller transmits global "turn off" signal to all devices on system. All devices cease operation.
17
Does system owner want to re-enable all devices on system?
No
Yes
18
Owner disconnects unauthorised device from system and enters system security code on controller. Controller transmits global "turn on" instruction to devices. All devices are re-enabled and operate normally.
END
END
END

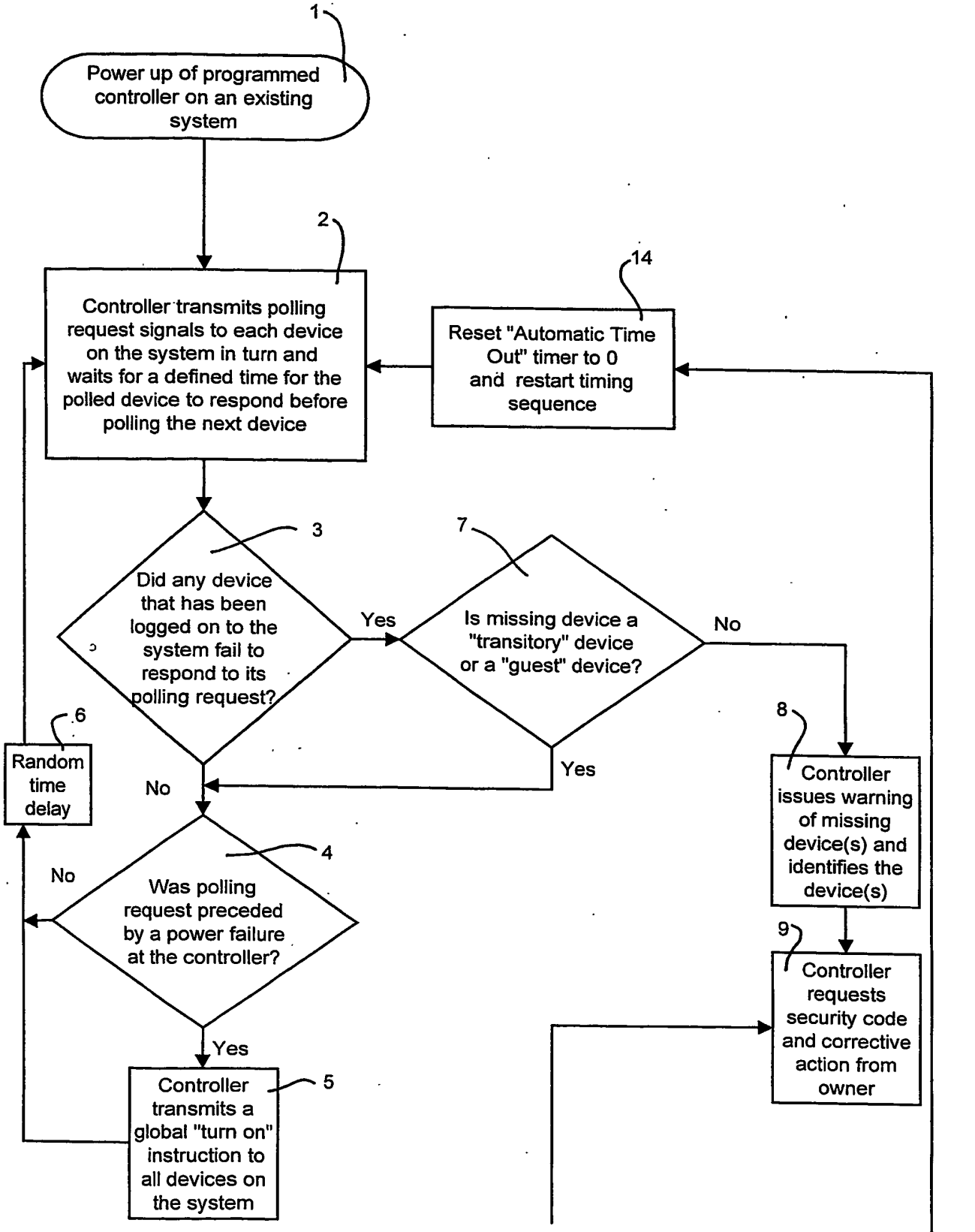

1
Power up of programmed controller on an existing system
2
Controller transmits polling request signals to each device on the system in turn and waits for a defined time for the polled device to respond before polling the next device
14
Reset "Automatic Time Out" timer to 0 and restart timing sequence
3
Did any device that has been logged on to the system fail to respond to its polling request?
Yes
7
Is missing device a "transitory" device or a "guest" device?
No
Yes
No
6
Random time delay
8
Controller issues warning of missing device(s) and identifies the device(s)
9
Controller requests security code and corrective action from owner
4
Was polling request preceded by a power failure at the controller?
No
Yes
5
Controller transmits a global "turn on" instruction to all devices on the system
From 11
From 10

FIG 5

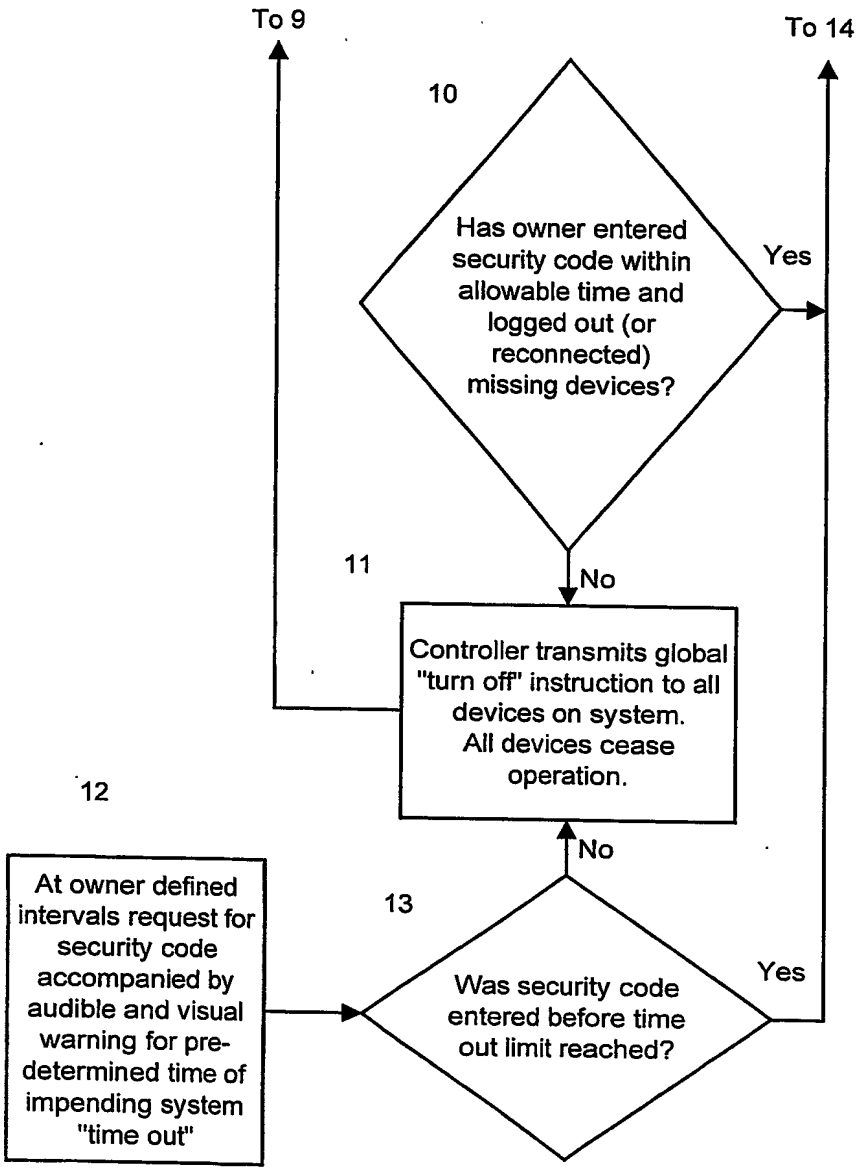

To 9
To 14
10
Has owner entered security code within allowable time and logged out (or reconnected) missing devices?
Yes
No
11
Controller transmits global "turn off" instruction to all devices on system. All devices cease operation.
12
At owner defined intervals request for security code accompanied by audible and visual warning for pre-determined time of impending system "time out"
13
Was security code entered before time out limit reached?
Yes
No

FIG 5 (cont)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00940

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G08B 13/22, G08B 13/00, G08C 17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, USPTO, ESPACE: G08B/IC, G08C/IC, G06F/IC & KEYWORDS: PLC, PLD, PROGRAMM+, CONTROLLER, THEFT, etc, SECURE+, ABLE, DISABLE, POWER, CABLE, LINE, APPLIANCE, ELECTRONIC, WHITE, ELECTRONIC, HI-FI, VCR, DVD, MICROWAVE, +PHONE?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	WO 96/36953 A (P-SERV TECHNOLOGIES PTE LTD) 21 November 1996	
X	Entire document	1-7, 12-14, 18-25
Y	Entire document	8-11, 15-17
	GB 2286277 A (LE GROUP VIDEOTRON LTEE) 9 August 1995	
X	Entire document; see abstract, drawings	1, 13, 14
Y	Entire document	2-12, 15-25
	GB 2259172 A (CHIU SING CHOY) 3 March 1993	
X	Entire document; see abstract, drawings	1, 13, 14
Y	Entire document	2-12, 15-25

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2003	- 1 SEP 2003
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	CHARLES BERKO Telephone No : (02) 6283 2169

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00940

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 392872 A (MOLEX INCORPORATED) 12 April 1990 Entire document; see abstract, drawings Entire document	1, 13, 14 2-12, 15-25
P, X P, Y	US 6542076 B (JOAO) 1 April 2003 Entire document; see abstract, drawings Entire document	13, 14 1-12, 15-25
X Y	WO 2002/11903 A (STEPHEN-DALY) 7 February 2002 Entire document; see abstract, drawings Entire document	13, 14 1-12, 15-25
X Y	US 6111504 A (PACKARD ET AL.) 29 August 2000 Entire document; see abstract, columns 2, 5. Entire document	13, 14 1-12, 15-25
Y	WO 2001/57627 A (CIRRUS LOGIC INC.) 9 August 2001 Entire document	1-25
Y	GB 2303726 A (COLLINS et al.) 26 February 1997 Entire document	1-25
Y	GB 2155708 A (FRANCIS et al.) 25 September 1985 Entire document	1-25
Y	US 5767771 A (LAMOUNT) 16 June 1998 Entire document	1-25
Y	EP 206483 A (BLACK & DECKER INC.) 7 May 1986 Entire document	1-25

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00940

Box I **Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos :

because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos : **26**

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The claim to a computer program, as directed, is vague and invites speculation as to exactly what features are covered by the monopoly sought.

3. ☐ Claims Nos :

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box II **Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU03/00940

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	9636953	AU	57868/96	CN	1185852	SG	45097
GB	2286277	BE	1008741	CA	2140968	DE	19503761
		FR	2716027	IT	MI 950158		950158
		IT	1273476	JP	8214376	NL	9500169
		PT	101648	US	5629868		
GB	2259172	NONE					
EP	392872	JP	2005896	AU	30153/89	EP	330374
US	6542076	US	5513244	US	5917405	US	2002121969
		US	2003016130	US	6549130	US	2003071899
WO	200211093	AU	20009029	AU	200176164	CA	2416079
		EP	1320840				
WO	200157627	AU	200131162	AU	200131164	AU	200131165
		AU	200134611	AU	200134678	EP	1256056
		EP	1256060	EP	1256061	EP	1256041
		EP	1258005	WO	200157657	WO	200157676
		WO	200157677	WO	200157872		
US	6111504	NONE					
GB	2303726	NONE					
GB	2155708	GB	2187018				
US	5767771	NONE					
EP	206483	AU	58588/86	CA	1260100	CA	1274890
		FR	2583552	JP	61288297	US	4755792

END OF ANNEX